UNIVERSIDADE DA CORUÑA

Guia docente				
Datos Identificativos				2023/24
Asignatura (*)	Test de Intrusión		Código	614530110
Titulación	Máster Universitario en Ciberseguridade			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero	Obligatoria	5
Idioma	CastellanoGallego			
Modalidad docente	Presencial			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación			
Coordinador/a	Carballal Mato, Adrián	Correo electrónico	adrian.carballal@udc.es	
Profesorado	Carballal Mato, Adrián Vázquez Naya, José Manuel	Correo electrónico	adrian.carballal@udc.es jose.manuel.vazquez.naya@udc.es	
Web	moovi.uvigo.es			
Descripción general	No hay una mejor forma de probar la fortaleza de un sistema que atacarlo. Los Test de Intrusión sirven para reproducir intentos de acceso de un atacante valiéndose de las vulnerabilidades que puedan existir en una determinada infraestructura. En este curso se cubrirán los temas fundamentales orientados a los test de intrusión (pentesting) cubriendo las distintas fases de un ataque y explotación (desde el reconocimiento y el control de acceso hasta el borrado de huellas).			

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A30	HD-10 - Identificar y aprovechar, de manera analítica y práctica, vulnerabilidades de los sistemas de información, así como identificar posibles vectores de ataque e innovar en técnicas y procesos referidos al hacking ético
B26	K-10 - Diferenciar los vectores y técnicas de ciberataque más comunes, así como comprender y aplicar los métodos y técnicas de detección de vulnerabilidades en equipos informáticos, redes de comunicaciones, bases de datos, programas y/o servicios de información
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C13	C-08 - Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético
C14	C-09 - Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal
C15	C-10 - Diseñar y gestionar la seguridad de infraestructuras para realizar la auditoría de seguridad de la infraestructura y garantizar continuidad de negocio bajo normas y estándares de referencia

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Identificar los riesgos y vulnerabilidades de un sistema de información	AP30		
Identificar los mecanismos de seguridad y su integración en las organizaciones	AP30		CP11
Utilizar herramientas de seguridad			CP13
Enfrentarse a casos reales y saber lo que hay que hacer en el menor tiempo posible			CP13 CP15
Capacidad de análisis y síntesis	AP30	BP26	CP14

Contenidos	
Tema	Subtema

Fundamentos	Hacking ético Vulnerabilidades Vectores de ataque Tipos de Test de Intrusión Alcance y objetivos
Estrategias de reconocimiento	Pasivo vs Activo Scapy P0f Netdiscover
Estrategias ofensivas	Análisis de vulnerabilidades Explotación de vulnerabilidades Elevación de privilegios Mantenimiento de acceso Pivoting
Métodos de evasión	Contramedidas Borrado de huellas

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	C15	9	13.5	22.5
Análisis de fuentes documentales	C11	6	6	12
Prueba de respuesta múltiple	B26	1.5	0	1.5
Prácticas de laboratorio	C11 C13 C14	6	12	18
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Prácticas de laboratorio	C11 C13 C14	4	8	12
Estudio de casos	A30 C13	5	6	11
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	Descripción
Sesión magistral	Transmisión de información y conocimiento clave de cada uno de los temas. La participación de los estudiantes se fomenta en ciertos momentos. Como parte de la metodología, un enfoque crítico de la disciplina llevará a los estudiantes a reflexionar y descubrir las relaciones entre los diferentes conceptos, formar una mentalidad crítica para enfrentar los problemas y la existencia de un método, facilitando el proceso de aprendizaje en el alumno. Para luchar contra la posible pasividad del alumno, en pequeños momentos se presentan pequeñas preguntas, que reflexionan sobre el alumno, complementando esos aspectos con referencias bibliográficas que le permiten enriquecer el conocimiento adquirido. Este intercambio con el alumno, como parte de la lección magistral, nos permite controlar el grado de asimilación del conocimiento por parte de él. Las lecciones magisteriales incluyen, tanto conocimiento extraído de las referencias de la asignatura, como los resultantes de nuestras propias experiencias profesionales, fomentando la capacidad del análisis crítico. En todo momento se busca que una cierta parte de los contenidos no requiera que el alumno los memorice. Esta metodología intentará lograr un alto grado de motivación en el alumno.

Análisis de fuentes documentales	Lectura y examen crítico de los principales documentos éticos de la informática. Sirven como una introducción general a los temas. Proporcionan una explicación histórica y sistemática de su significado. Son de gran importancia en el contexto de las otras metodologías utilizadas en el tema.
Prueba de respuesta múltiple	Esta prueba estará orientada a determinar si el alumno ha asimilado los diferentes objetivos de la asignatura.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Prácticas de laboratorio	Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.
Estudio de casos	El análisis ético y legal de la tecnología de la información tiene características específicas. Con el estudio de caso, se pretende examinar la estructura y el contenido de los problemas presentes en los casos, tanto individualmente como en grupos. Es una forma de aprendizaje de contenido y también metodológica, en la cual el alumno aprende a analizar, deliberar y llegar a conclusiones razonables y razonables con los argumentos éticos y legales. Es muy útil para ejercitar las habilidades y las habilidades argumentativas.

Atención personalizada	
Metodologías	**Descripción**
Prácticas de laboratorio Prácticas de laboratorio Prácticas de laboratorio Prácticas de laboratorio Prácticas de laboratorio Prácticas de laboratorio	Prácticas de laboratorio: se guía al alumno individualmente en el desarrollo de cada una de las prácticas de laboratorio. Aunque en el desarrollo de la primera práctica existen grandes diferencias en las necesidades de cada alumno, se están homogeneizando progresivamente en términos de sus necesidades de atención personalizada. Sin duda, la identificación de este parámetro es fundamental para determinar que la totalidad de los estudiantes avanza durante el desarrollo de la asignatura. También haremos que los grupos pequeños trabajen juntos en desarrollos prácticos. Atención personalizada: cualquier pregunta tecnológica expuesta por el alumno, en persona, tutoriales, correo electrónico, etc. En caso de detección de plagio en cualquiera de las pruebas (pruebas cortas, exámenes parciales o examen final), la calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos. En todas las convocatorias (primera oportunidad, segunda oportunidad y convocatoria extraordinaria) se realizará una evaluación única tanto en la parte práctica como en la teórica.

Evaluación			
Metodologías	Competencias / Resultados	Descripción	**Calificación**
Prácticas de laboratorio	C11 C13 C14	Practica 2: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 3: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 4: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 5: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10
Prácticas de laboratorio	C11 C13 C14	Practica 6: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10
Prueba de respuesta múltiple	B26	Esta prueba incluye los contenidos y, en general, todos los aspectos relacionados con los objetivos de la asignatura. Establece varios temas relacionados tanto con el contenido de las sesiones maestras como con las prácticas de laboratorio, dando más peso al primero. Es necesario obtener una calificación promedio superior a 4 para hacer media.	40
Prácticas de laboratorio	C11 C13 C14	Practica 1: Cada alumno de prácticas de laboratorio deberá realizar una prueba de penetración sobre una máquina virtual preconfigurada por el profesorado. El alumno dispondrá de un calendario determinado para la resolución de la misma, y en los casos donde dicho calendario no se cumpla la nota de dicha practica será penalizada. El alumno deberá presentar un documento que acredite a los pasos realizados para el desempeño de la práctica.	10

Observaciones evaluación

OPORTUNIDAD ORDINARIA

Siguiendo las directrices de la titulación, a quienes cursen esta asignatura se les ofrecerán dos sistemas de evaluación: evaluación continua y evaluación global. Al finalizar el primer mes de curso, los alumnos deberán indicar a los profesores de la asignatura el sistema de evaluación elegido. Quienes opten por el sistema de evaluación continua no podrán ser calificados como ?no presentados? si realizan una entrega o prueba de evaluación con posterioridad a la notificación de su decisión.

Sistema de evaluación continua

Los alumnos que opten por el sistema de evaluación continua deberán:

-Realizar seis prácticas de laboratorio de ensayos de penetración. El alumno dispondrá de un calendario específico para la resolución de las mismas, y en los casos en que no se cumpla dicho calendario, se penalizará la nota de dicha práctica. Estas pruebas supondrán el 60% de la calificación global de la asignatura, un 10% cada una.

- Realizar una prueba de respuesta múltiple sobre los contenidos de las clases expositivas y prácticas de laboratorio. Esta prueba supondrá el 40% de la calificación global de la asignatura y es necesario sacar un mínimo de 4 sobre 10 para aprobar la asignatura.

La nota global de la asignatura será igual a la suma de las tareas indicadas. Para aprobar la asignatura, la calificación global deberá ser mayor o igual a cinco.

Sistema de evaluación global

Los estudiantes que opten por el sistema de evaluación al final del semestre deberán:

- Realizar una prueba de penetración dada en un tiempo definido por los profesores. Esta prueba supondrá el 60% de la nota global de la asignatura.
- Realizar una prueba de respuesta múltiple sobre los contenidos de las clases expositivas y prácticas de laboratorio. Esta prueba supondrá el 40% de la calificación global de la asignatura y es necesario sacar un mínimo de 4 sobre 10 para aprobar la asignatura.

La nota global de la asignatura será igual a la suma de las tareas indicadas. Para aprobar la asignatura, la calificación global deberá ser mayor o igual a cinco.

OPORTUNIDAD EXTRAORDINARIA

Sólo aquellos alumnos que no se presentaron o reprobaron la materia en la oportunidad ordinaria podrán presentarse a la evaluación en la oportunidad extraordinaria.

La evaluación consistirá en la realización de una o dos de las siguientes tareas, en función de la calificación obtenida previamente en las pruebas equivalentes de la oportunidad ordinaria:

- Realizar una prueba de penetración dada en un tiempo definido por los profesores. Esta prueba supondrá el 60% de la nota global de la asignatura.
- Realizar una prueba de respuesta múltiple sobre los contenidos de las clases expositivas y prácticas de laboratorio. Esta prueba supondrá el 40% de la calificación global de la asignatura y es necesario sacar un mínimo de 4 sobre 10 para aprobar la asignatura.

En el caso de que la nota en las pruebas de oportunidad ordinaria, equivalentes a éstas, sea superior o igual a cinco, el alumno podrá optar por mantener su nota de oportunidad ordinaria o volver a presentarse a la prueba.

OTROS COMENTARIOS

-Las puntuaciones obtenidas sólo son válidas para el curso académico en curso.

- El uso de cualquier material durante los exámenes y pruebas de evaluación deberá ser autorizado expresamente por el profesorado de la asignatura.

-En caso de detección de copia en alguna de las pruebas (pruebas cortas, exámenes parciales o examen final), la nota final será SUSPENSIÓN (0) y se comunicará el hecho a la dirección del Centro a los efectos oportunos.

Fuentes de información	
Básica	- Mike Schiffman (2001). Hacker's Challenge. Osborne - Pablo Gonzalez Perez, Germán Sánchez Garcés, Jose Miguel Soriano de la Cámara (2013). Pentesting con Kali. 0xWORD - Julio Gomez López, Miguel Angel de Castro Simón, Pedro Guillén Núñez (2014). Hackers, Aprende a atacar y a defenderte. RA-MA - David Puente Castro (2013). Linux Exploiting. 0xWORD - Pablo Gonzalez Perez (2016). Metasploit para Pentesters. 0xWORD - Crystal Panek; Robb Tracy (2019). CompTIA pentest+ practice tests : exam PT0-001. Independiente - María Ángeles Caballero Velasco, Diego Cilleros Serrano (2022). El libro del Hacker. Edición 2022. Anaya

Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Seguridad de la Información/614530003 Redes Seguras/614530006
Asignaturas que se recomienda cursar simultáneamente
Conceptos y Leyes en Ciberseguridad/614530001 Ciberseguridad en Entornos Industriales/614530014
Asignaturas que continúan el temario
Trabajo Fin de Máster/614530017 Gestión de la Seguridad de la Información/614530002
Otros comentarios
- Según se recoge en las distintas normativas de aplicación para la docencia universitaria deberá incorporarse la perspectiva de género en esta materia (se usará lenguaje no sexista, se utilizará bibliografía de autores/as de ambos sexos, se propiciará la intervención en clase de alumnos y alumnas...)- Se trabajará para identificar y modificar perjuicios y actitudes sexistas y se influirá en el entorno para modificarlos y fomentar valores de respeto e igualdad.- Deberán detectarse situaciones de discriminación por razón de género y se propondrán acciones y medidas para corregirlas.